

Local Hamiltonians with No Low-energy Trivial States

Lior Eldar*

Aram W. Harrow*

October 27, 2015

Abstract

We prove the NLTS (No Low-energy Trivial States) conjecture of Freedman and Hastings [22]: we construct an explicit infinite family of 7-local commuting Hamiltonians such that any quantum state that has only locally-generated entanglement has high energy w.r.t. the Hamiltonian, and this energy scales linearly in the number of local terms.

From a complexity-theoretic viewpoint, since an existence of a quantum PCP theorem implies NLTS our result may be seen as the first evidence in favor of a quantum PCP.

From a purely quantum-mechanical perspective, our result implies for the first time the existence of locally-defined Hamiltonians, albeit with long-range interactions, with the following property of “robust entanglement”: applying to the ground-space of the Hamiltonian any error that generates a sufficiently small constant fractional energy cannot destroy its multi-particle entanglement, in a well-defined sense. This suggests that the apparent fragility of multipartite entanglement is essentially an artifact of considering local Hamiltonian systems which are not only local but *spatially local*.

Our Hamiltonian is based on applying the Tillich-Zémor product code [41] to a classical locally testable code such as the Hadamard code - as in [20]. A key tool in our proof is a new lower bound on the vertex expansion of the output of low-depth quantum circuits.

1 Introduction

1.1 Background and main result

1.1.1 Multipartite entanglement, trivial states and topological order

Quantum mechanics has overturned our classical intuitions about the nature of information, computing and knowledge. Perhaps the greatest departure from earlier notions of information is the phenomenon of entanglement, which implies that describing the state of many particles cannot be reduced to a probabilistic mixture of descriptions of the state of each individual particle. For decades, entanglement was viewed in terms of its counterintuitive properties, e.g. the Bell and GHZ “paradoxes,” and only in recent years has quantum information theory begun a systematic program of quantifying, characterizing and finding ways to test entanglement.

However, in typical many-body systems, and from a complexity-theoretic point of view, the important question is not whether or not there is entanglement, but whether it is short-range or long-range. Many of the results of quantum information theory apply to the case of bipartite entanglement and often do not extend to this setting of large numbers of interacting systems. For example, a collection of $n/2$ singlets has high bipartite entanglement across most

*Center for Theoretical Physics, MIT

cuts but this entanglement is in a certain sense “local” and could be eliminated by a suitable coarse-graining.

The concept of a “trivial state” is meant to express the notion that states such as $n/2$ singlets have only short-range entanglement. A trivial state is (informally) a state that can be prepared from a product state by a $O(1)$ -depth quantum circuit, or roughly equivalently, by an $O(1)$ -time evolution under a Hamiltonian that is a sum of local terms with bounded norm. This is a special case of a more general classification of quantum phases in which two states are said to be equivalent if they differ by an $O(1)$ -depth quantum circuit [18]; here trivial states correspond to the phase that includes product states. Nontrivial states are sometimes said to be topologically ordered, and examples include code states of the toric code, or indeed any QECC with distance more than a constant [15]. “Topological order” is an imprecisely defined term that we will not do justice to here, but trivial states have been shown to be equivalent to states without [various versions of] topological order in [15, 24, 31, 40, 30].

1.1.2 The quantum-mechanical perspective: robustness of entanglement

Arguably, the biggest barrier to building a quantum computer is the fact that long-range entanglement, i.e. the type that could be useful to solve hard computational problems, e.g. in Shor’s algorithm, is quantum decoherence by which highly entangled states decohere into classical distributions of trivial states, by interacting with the environment. While quantum data can be encoded in ways that protect against damage to a constant fraction of subsystems, all known such codes cannot be even verified without entangling measurements on an asymptotically growing number of systems. In terms of a closed physical system, this suggests that the quantum states that inhabit the low side of the spectrum of a physical Hamiltonian, contain numerous trivial, non-quantum states. In other words, even quantum states whose energies are a vanishingly small fraction of the total available energy, can already be completely trivial.

Until now theoretical, and even more so, experimental realization of quantum-mechanical systems (i.e. local Hamiltonians) all have trivial states at vanishingly small energies. In a sense, this is no surprise, as these systems have been based on embedding qubits in a low-dimensional grid which, by definition has trivial states with arbitrarily small energy. These are the quantum states that are tensor products of local states that each satisfy a small constant-size box of the grid. Such states have energy which is at most the penalty by the Hamiltonians at the boundary of these boxes, which can be made an arbitrarily small constant.

Hence, the above problem raises a more fundamental question regarding quantum entanglement: could it be that our notion that entanglement is fragile is merely an artifact of building systems in low-dimensional grid? Could it be that, at least theoretically, quantum systems defined on more highly connected topologies could have entanglement which is more resilient? This question was formulated rigorously by Freedman and Hastings [22] and was called the NLTS conjecture (see definition 13). Loosely stated, it calls for local Hamiltonians for which any quantum state that has energy, say at most $1/10$ of the total available energy, is highly entangled.

Several works around the NLTS conjecture, and its parent conjecture (quantum PCP - see next section) have provided ambiguous evidence about its ultimate status. Indeed, the works of [16, 13, 28, 7] have suggested that the NLTS conjecture may be false by showing that large classes of local Hamiltonians have trivial states at very low energies. In other words, even quantum systems that are very far from being defined on a low-dimensional grid suffer from the same problem of having low-energy trivial states.

Despite these negative results we provide an affirmative answer to the NLTS conjecture by constructing an infinite family of local Hamiltonians in which any quantum low-energy state has long-range entanglement:

Theorem 1. (Informal) *There exists an explicit family of Hamiltonians $\{H_n\}_n$, each with $0 \leq H_n \leq I$,*

and H_n a sum of commuting 7-qubit terms, such that any quantum state $|\psi_n\rangle$ with $\langle\psi_n|H_n|\psi_n\rangle \leq \varepsilon$ cannot be even approximately simulated (in terms of a probability distribution induced by a tensor-product measurement) by quantum states with depth $o(\log(n))$.

This implies that our notion that entanglement is a fragile phenomenon, i.e. that local Hamiltonians have trivial states with vanishingly small energy, is possibly an artifact of embedding these Hamiltonians on a spatially-local grid.

Technically speaking our result is about the robust *testability* of entanglement, and in particular, of the property of being nontrivial. There has been a major research effort towards understanding *entanglement witnesses*, which can be thought of as real-valued functions on density matrices for which $f(\sigma) \geq 0$ for all separable σ and $f(\rho) < 0$ for some entangled ρ . In general entanglement witnesses do not separate all entangled states from all separable states, but rather we can think of f being chosen in a way that depends on the state ρ (or a small family of such states) whose entanglement we would like to witness. As a result, such witnesses can be admirably simple, as in the famous Bell test which requires only local measurements and classical post-processing.

Our result can be viewed in this context as a *robust non-triviality witness*. The Hamiltonian H_n is an observable which satisfies $\text{tr}[H_n\sigma] \geq \varepsilon$ for all trivial states σ and $\text{tr}[H_n\rho] = 0$ for at least one state ρ . The “robust” property means that non-triviality can be (probabilistically) witnessed by measuring only the 7 qubits in a randomly chosen clause. Like the tests used in the PCP theorem, a true ground state will always pass this test and any trivial state will have $\Omega(1)$ probability of failing it.

1.1.3 The complexity-theoretic perspective: the quantum PCP conjecture

Another motivation for studying trivial states comes from complexity theory. The Local Hamiltonian problem is to estimate the ground-state energy (lowest eigenvalue) of a Hamiltonian that is specified as a sum of terms each acting on a constant number of qubits. It is the quantum analogue of a CSP (constraint satisfaction problem). Analogously, a key result in quantum complexity theory is that the Local Hamiltonian problem is complete for the complexity class QMA in the regime where energy must be approximated to precision $1/\text{poly}(n)$ for n qubits [32]. The class QMA is the quantum analogue of NP in which the proof consists of a quantum state and the verifier has a quantum computer to check its validity [42]. Questions related to the complexity of the Local Hamiltonian problem have grown into a new area at the intersection of complexity theory and condensed matter physics known as quantum Hamiltonian complexity [37].

A major open question in this field is the quantum PCP (probabilistically checkable proof) conjecture [1, 4]. The classical PCP is, arguably, the crowning achievement in computer science in the last 20 years. It states [9, 10, 19] that it is NP-hard to distinguish between completely satisfiable instances local constraint satisfaction, and instances in which any assignment disagrees with a good fraction of the constraints. By contrast, the original Cook-Levin theorem shows only that it is NP-hard to distinguish a satisfiable boolean formula from one in which *at least one* clause must be unsatisfied by any assignment.

The quantum PCP (qPCP) conjecture [1, 4] asserts that it is QMA-complete to approximate the Local Hamiltonian problem up to error εm , where m is the number of terms in the Hamiltonian and we assume each term has norm ≤ 1 . This “PCP-style” error scaling can be thought of as “constant energy density,” meaning that the energy error we allow is proportional to the maximum possible energy in the system. This is the situation that we have e.g. for thermal state at constant temperature $T > 0$.

This problem is at least NP-hard thanks to the classical PCP theorem and it is also contained in QMA. The difference between these classes can be thought of as the difference in utility between a quantum state and a classical description of a quantum state. If the quantum PCP

theorem were true and assuming a separation of the form $\text{MA} \subsetneq \text{QMA}$ then it would mean that some Hamiltonians could not have their low-energy states described by any efficiently verifiable classical string. Finding such succinct descriptions is a central project of theoretical physics, and a complexity-theoretic barrier to it would suggest that certain types of knowledge (e.g. about low-energy states of Hamiltonians) can be communicated quantumly but not classically.

The NLTS conjecture described above is, therefore, a necessary condition for quantum PCP to hold, assuming $\text{MA} \subsetneq \text{QMA}$. Hence, if one were to refute NLTS it would imply that there is no hope for quantum PCP. Therefore, by proving the NLTS conjecture we have, in a sense, indicated that quantum PCP may be possible, despite all previous negative results. Still, it remains a tough problem, since one would not only need to devise a robust form of entanglement but one which is also useful for encoding QMA-hard problems.

1.2 Proof outline

We begin in Section 4 by defining a “complexity witness,” meaning a simple-to-verify property that can prove a state is nontrivial. In particular, we show in Section 4 that measuring a trivial state in any product basis results in a probability distribution over $\{0, 1\}^n$ with high expansion. It is well known that the uniform measure on $\{0, 1\}^n$, or indeed any product measure, has good expansion properties. It is not hard to see this is also true for the output of low-depth classical circuits. We extend this to quantum circuits, by using Chebyshev polynomials in a way inspired by [23, 8].

We refer to non-expanding distributions as “approximately partitioned”; meaning that we can identify two well-separated subsets S_0, S_1 each with large mass. A prototypical example of a state giving rise to an approximately partitioned distribution is the cat state $|0^n\rangle + |1^n\rangle$. However, the cat state is not the unique ground state of any local Hamiltonian [17]. The uniform distribution of any (classical) code with good distance is approximately partitioned, but simply using the check operators of a classical code is insufficient since computational basis states are also trivial states. A state which combines both of the above desirable features is the state of a quantum error correcting code (QECC). Since QECCs protect encoded information by spreading it out over a much larger Hilbert space, they are natural candidates for creating robust forms of entanglement. We will show in Section 5 the “warm-up” result that Hamiltonians corresponding to a special subclass of QECCs (namely CSS codes) have no *zero-energy* trivial states. (Some version of this claim was folklore [15, 24].) Here if we want to consider local Hamiltonians then it is necessary to restrict to codes with low-weight check operators, also known as LPDC (low-density parity-check) codes.

Later we will construct a quantum code in Section 8 that is robust, meaning that even states that violate a small constant fraction of constraints should in some sense still be close to the code space. We will use a CSS (Calderbank-Shor-Steane; cf. Section 2) code, so we can measure “close” in terms of the distributions obtained when measuring in the X or Z bases.

Our code will have two ingredients: 1) a classical LTC (locally testable code), and 2) the Tillich-Zémor code product, reviewed in Section 7. The classical LTC is what gives us robustness. Classically, an LTC has the property that a word violating a small fraction of constraints is close to some codeword.

The Tillich-Zémor code product [41] gives a method for embedding a classical code into a CSS code. It does not preserve distance, so for example, its best distance parameter scales like $O(\sqrt{N})$ for N qubits, whereas we are interested in protecting against a linear number of errors, i.e. $\Omega(N)$. However, one lesson from our work is that distance may not always be the best measure for how well a quantum code resists error in the context of NLTS. As it turns out, there exists a subset of the logical words of the quantum product code that is isomorphic to the original LTC. While these words have weight only $O(\sqrt{n})$ each, they also inherit some form of

local testability from the underlying classical LTCs.

Next, we note that even a residual form of local testability does not imply that a low-energy quantum state is hard to generate. In particular, classical bit-string assignments are trivially easy to generate. Here, we make use of the fact the quantum uncertainty principle. The fact that we use a quantum code means we can measure in either the X or Z basis. A standard uncertainty argument means that at least one of these should have high uncertainty. This is what lets us get around the limitation of classical codes and lets us put a lower bound on how dispersed the distribution is. In this context, the distance and local testability of the original LTC will imply that at least in one of the X or Z basis, the measured distribution must be approximately partitioned, and therefore that the state must be nontrivial.

On the way to our final result we show in Section 6, as a second “warm-up,” that quantum LTCs [6] have the NLTS property. While we do not know if qLTCs exist (the codes we construct in this paper are not examples of qLTCs), this demonstrates many of the key ideas of our main proof. Finally we show in Section 9 that our Hamiltonians have the NLTS property. The proof is more difficult than for the case of qLTCs because our codes have a feature like that of subsystem codes: only some of the logical degrees of freedom can be said to be protected by the local testability condition.

1.3 Previous Work

Most of the previous results established various settings in which NLTS was known not to hold. In the following list we identify Hamiltonians with the [hyper-]graph in which each qubit is a vertex and each interaction term defines a [hyper-]edge.

1. Non-expanding graphs, including $O(1)$ -dimensional lattices. This was folklore and holds even classically, but was formalized in [13].
2. Graphs where most vertices have $\omega(1)$ degree [13].
3. 2-local Hamiltonians with commuting terms [16].
4. 3-qubit Hamiltonians with commuting terms [5].
5. Sparse commuting $O(1)$ -local Hamiltonians corresponding to graphs with high girth [28].
6. Commuting $O(1)$ -local Hamiltonians with high local expansion [7].

The above results rule out topologies (such as high-degree graphs) which are known to be compatible with classical PCP constructions. This combination of constraints (degree and expansion must be high but not too high, etc.) made it plausible that NLTS would be false, at least in the commuting case. Indeed Ref. [13] shows that if the gap-amplification step of Dinur’s PCP theorem [19] worked quantumly (as was proposed by [3]), it would actually *refute* the qPCP conjecture.

Our result will have to dodge the above no-go theorems by employing a Hamiltonian (a) on an expanding hypergraph, (b) albeit one with $O(1)$ degree, (c) by being 7-local (although the terms do commute), and (d) by having much smaller local expansion than one would expect from a random graph (and specifically not being hyper-finite, in the language of [22]).

We also review the various incomplete attempts at establishing NLTS:

1. The cat state is nontrivial but not the ground state of any local Hamiltonian [17].
2. Freedman and Hastings [22] give an example with “one-sided NLTS.” Here the Hamiltonian contains X and Z terms and has the property that a state which satisfies most of the X terms and all of the Z terms must be nontrivial.
3. The uniform distribution over the code space of a classical code can be shown to require $\Omega(\log(n))$ depth to produce. (This is a new result of ours but not hard to prove, and arguably was implicit in previous work [15, 24].) If the code is an LDPC (low-density

parity check) then this can be verified with $O(1)$ -weight checks. If it is an LTC (locally testable code; see main paper for details), then this claim becomes robust, i.e. it requires $\Omega(\log(n))$ depth to produce a distribution that even approximately matches the desired distribution. However, there is no way with classical constraints to force the distribution to be uniform. A single string in the support of the code space can be prepared in depth 1. Only in a quantum code with both X and Z terms can we require a state to be in superposition. Thus the conjecture is inherently quantum. However, we will make some use of the classical intuition here.

Aside from the above no-go results on NLTS, we would like to relate to the recent work of [33] on quantum codes. That work provided the first known example of a quantum code on n qubits with $n^{\Omega(1)}$ distance and a decoder that runs in time $O(n)$. The construction applies the hyper-graph product to a pair of bipartite expander codes.

As stated above, however, such a construction is probably not robust: w.h.p. over the choice of underlying classical codes, these codes will not be locally testable. This implies that the product of these codes, e.g. the resulting quantum CSS code, will have code-states that are very far from the code-space in terms of Pauli Hamming distance, yet their energy w.r.t. the Hamiltonian would be very small. In such a scenario, where one can generate linear combinations of states with high error weight but with low energy w.r.t. the Hamiltonian, it is plausible that one can find trivial states that approximate the ground-energy of the Hamiltonian. This reinforces the importance of the local-testability property both in the classical and quantum setting, and its apparent connection to robust forms of quantum entanglement.

In [20] the construction described in this paper was used to show lower bounds on the *classical* circuit depth, with bounded fan-in/fan-out required to simulate low-energy states. This result subsumes [20] as it proves a general lower bound for quantum circuits based on approximate partitions. This tool may be of use for proving quantum circuit lower bound in other settings.

1.4 Discussion and Open Questions

NLTS is a weaker conjecture than both qPCP and qLTC, assuming $\text{MA} \subsetneq \text{QMA}$. After a series of papers containing only bad news for the qPCP and qLTC conjectures, this result can be seen as a pro-qPCP/qLTC development.

However, our code is not a qLTC. Here is a counter-example to the proof that \mathcal{C}_\times is restricted qLTC: consider the string z which is a proper codeword of \mathcal{C} in each column of $V \times V$, and in $C \times C$ you have a string of large weight. Then because we have no promise on the qLTC behavior of C^T it may very well be that the restriction of z to $C \times C$ (i.e. taking the restriction of each check term to $C \times C$) has very few violations on H_x . (see e.g. [11]). Since the restriction of H_x to $V \times V$ has 0 violations by the assumption above, it implies that $H_x \cdot z$ has low weight, despite z being far from the code.

Another open question is how we can find circuit depths lower bounds beyond $\log(n)$, or for spatially local circuits, beyond the point at which their blowup becomes n . Not only do our expansion lower bounds break down at this point, but in fact all stabilizer states can be prepared in $O(\log(n))$ depth [2]. Probabilistic arguments (cf. [14]) can establish a loose depth hierarchy for quantum circuits: circuits of depth n^k cannot distinguish random circuits of depth n^{11k+9} from Haar-random circuits. But it would be more useful to have concrete methods for lower bounding depth at levels above $\log(n)$.

Finally the qPCP conjecture is a natural next target. One challenge is that there exists an NP witness for the ground-state energy of a commuting Pauli Hamiltonian, making use of the Gottesman-Knill theorem [2]. Of course our Hamiltonians do not encode any particular problem and always have ground-state energy 0. Moving beyond commuting Pauli operators will be one of many hurdles required to translate our result into a proof of the qPCP conjecture.

2 Preliminary facts and definitions

2.1 Notation

- $\|M\|$ is the operator norm of M , i.e. the largest singular value.
- For $x, y \in \{0, 1\}^n$, let $\text{dist}(x, y)$ denote their Hamming distance, i.e. the number of positions in which they differ. For sets $X, Y \subseteq \{0, 1\}^n$, define $\text{dist}(X, Y) = \min_{x \in X} \min_{y \in Y} \text{dist}(x, y)$. For a point $x \in \{0, 1\}^n$ and a set $Y \subseteq \{0, 1\}^n$ define $\text{dist}(x, Y) := \min_{y \in Y} \text{dist}(x, y)$. In general we identify $\{0, 1\}^n$ with \mathbb{F}_2^n and in particular use $x + y$ to denote $x \oplus y$ whenever $x, y \in \{0, 1\}^n$.
- A probability distribution p on $\{0, 1\}^n$ is (η, D) -approximately partitioned if there exist sets S_1, S_2 with $\text{dist}(S_1, S_2) \geq D$ and $p(S_1) \geq \eta, p(S_2) \geq \eta$. We write simply *approximately partitioned* when $\eta = \Omega(1)$ and $D = \Omega(n)$.
- For subsets $A, B \subseteq \mathbb{F}_2^n$, let $A + B$ denote the set of all possible pairwise sums $x + y$ with $x \in A, y \in B$. In particular, when B has one element x , we may, omit the set notation and write $A + x$.
- For a linear subspace $A \subseteq \mathbb{F}_2^n$ over \mathbb{F}_2 , we denote by A^\perp , the dual of A as

$$A^\perp = \{x \in \mathbb{F}_2^n, \langle w, x \rangle = 0, \forall w \in A\}.$$

We say that $A \perp B$ if $A \subseteq B^\perp$ or equivalently if $B \subseteq A^\perp$.

- Let $C \subseteq \mathbb{F}_2^n$ be some code on n bits. The minimal distance of C , denoted by $\Delta_{\min}(C)$ is the minimal distance between any pair of unique words in the code

$$\Delta_{\min}(C) = \min_{x \neq y, x, y \in C} \text{wt}(x + y).$$

We also define the *relative* minimal distance of C by $\delta_{\min}(C) = \Delta_{\min}(C)/n$.

- Let \mathcal{C} be a parity-check code on n bits, defined by the Tanner graph $G = (V, C; E)$ where V correspond to the set of bits, C corresponds to the set of checks, and E is the set of edges where each check $c \in C$ is connected to all the bits it checks in V . The transpose of the code \mathcal{C} , denoted by \mathcal{C}^T , is defined by exchanging the roles of the bits, and checks, i.e. it is the code whose Tanner graph is $G = (C, V; E)$. If A_E is the adjacency matrix of E (with rows indexed by C and columns by V) then $\mathcal{C} = \ker A_E$ and $\mathcal{C}^T = \ker A_E^T$.
- Let $S, T, S \subseteq T \subseteq \mathbb{F}_2^n$ denote some linear subspaces. Then T/S denotes the quotient space, meaning the set of cosets $\{t + S : t \in T\}$. Also, $T - S$ denotes the set of strings in T that are not in S . In particular, T/S has a representation in terms of elements of $T - S$, and the 0 element (representing S).

2.2 Quantum codes and local Hamiltonians

Definition 2. Pauli operators

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (1)$$

For $e \in \mathbb{F}_2^n$, define $X^e = X^{e_1} \otimes X^{e_2} \otimes \dots \otimes X^{e_n}$, i.e. the tensor product of X operators in each position where $e_i = 1$; similarly define $Z^e = \bigotimes_i Z^{e_i}$.

Definition 3. CSS code

A quantum CSS code on n qubits is a subspace of the Hilbert space of n qubits. It is defined by a pair of linear subspaces of $S_x, S_z \subseteq \mathbb{F}_2^n$ such that $S_x \perp S_z$. It is thus denoted $\mathcal{C} = \mathcal{C}(S_x, S_z)$. Explicitly the subspace is given by

$$\mathcal{C}(S_x, S_z) = \{|\psi\rangle \in (\mathbb{C}^2)^{\otimes n} : X^x|\psi\rangle = |\psi\rangle \forall x \in S_x, Z^z|\psi\rangle = |\psi\rangle \forall z \in S_z\} \quad (2)$$

$$= \text{Span} \left\{ \frac{1}{\sqrt{|S_x|}} \sum_{x \in S_x} |z + x\rangle : z \in S_z^\perp \right\}. \quad (3)$$

We say that the code contains $\log(\dim \mathcal{C})$ logical qubits, with the spaces of logical X, Z operators respectively defined by the quotient spaces $S_z^\perp/S_x, S_x^\perp/S_z$. (The nontrivial X, Z operators are given by $S_z^\perp - S_x, S_x^\perp - S_z$, respectively.) The distance is the minimum weight of any element of $S_x^\perp - S_z$ or $S_z^\perp - S_x$.

Definition 4. k -local Hamiltonian

A k -local n -qubit Hamiltonian $H \succeq 0$ is a positive semidefinite operator on the n -qubit space $(\mathbb{C}^2)^{\otimes n}$, that can be written as a sum $H = \frac{1}{m} \sum_{i=1}^m H_i$, where each H_i is a positive-semidefinite matrix, $0 \preceq H_i \preceq I$, and each H_i may be written as $H_i = h_i \otimes I$, where $h_i \succeq 0$ is a $2^k \times 2^k$ matrix.

Note that some parts of our definition, such as the eigenvalue bounds, are more restrictive than those used elsewhere. However, these are used to set the scale with respect to which we will discuss notions such as “constant energy” and do not materially change our results.

Definition 5. The Hamiltonian of the code

Suppose $\mathcal{C} = \mathcal{C}(S_x, S_z)$ is a CSS code and H_x, H_z are subsets of \mathbb{F}_2^n that generate S_x, S_z . Then we can define a Hamiltonian $H(\mathcal{C})$, whose terms correspond to the generators of the CSS code in the following way.

$$H = H(\mathcal{C}) = \frac{1}{2|H_x|} \sum_{e \in H_x} \frac{I + X^e}{2} + \frac{1}{2|H_z|} \sum_{e \in H_z} \frac{I + Z^e}{2}. \quad (4)$$

Observe that the CSS condition $S_x \perp S_z$ implies that the terms of $H(\mathcal{C})$ all commute. Thus the ground subspace of $H(\mathcal{C})$ is precisely the code space \mathcal{C} . Moreover, if the generating sets H_x, H_z contain only terms with weight $\leq k$ then the corresponding Hamiltonian $H(\mathcal{C})$ is a k -local Hamiltonian. We can think of H as checking whether a state is a valid code state with the energy corresponding to a measure of distance from the code: no states have negative energy, the set of zero-energy states is precisely the set of valid code states, and otherwise the energy equals the expected fraction of constraints violated. However, in general the number of violated constraints may not correspond to more conventional notions of “distance,” such as (for classical strings) the Hamming distance to the nearest codeword. In the next section we discuss a type of code that addresses this.

2.3 Locally testable codes

Definition 6. Classical locally testable code

A code $C \subseteq \mathbb{F}_2^n$ is said to be locally testable with parameter ρ , if there exists a set of check terms $\{C_1, \dots, C_m\}$, such that

$$\text{Prob}_i [C_i(w) = 1] \geq \rho \cdot \frac{\text{dist}(w, C)}{n}.$$

In particular this means that the check terms verify membership in the code, i.e. $w \in C$ iff $C_i(w) = 0$ for all i .

Similarly, a quantum locally testable code can be defined by the property that states at distance d to the codespace have energy $\geq \Omega(d/n)$. (This normalization reflects the fact that the check Hamiltonian $H(\mathcal{C})$ has norm ≤ 1 .) Our definition is a slight variant of the one from [6].

Definition 7. If V is a subspace of $(\mathbb{C}^2)^{\otimes n}$ then define its t -fattening to be

$$V_t := \text{Span}\{(A_1 \otimes \cdots \otimes A_n)|\psi\rangle : |\psi\rangle \in V, \#\{i : A_i \neq I\} \leq t\}. \quad (5)$$

Let Π_{V_t} project onto V_t . Then define the distance operator

$$D_V := \sum_{t \geq 1} t(\Pi_{V_t} - \Pi_{V_{t-1}}). \quad (6)$$

This reflects the fact that for quantum states, Hamming distance should be thought of as an observable, meaning a Hermitian operator where a given state can be a superposition of eigenstates.

Definition 8. Quantum locally testable code

Given a Hilbert space \mathcal{H} , a quantum locally testable code $\mathcal{C} \subseteq \mathcal{H}$, with local projection checks C_1, \dots, C_m , and soundness constant $\rho > 0$, is a quantum code, such that for any quantum state $|\psi\rangle$ we have the operator inequality

$$H(\mathcal{C}) \succeq \rho \cdot \frac{D_{\mathcal{C}}}{n}.$$

For stabilizer codes (which we will exclusively study in this paper) this can be seen to be equivalent to the definition in [6]. However we believe it gives a more generalizable definition of quantum Hamming distance.

We now state the following connection (proved in Claim 3 of [7]) between classical and quantum CSS locally testable codes:

Fact 9. Classical codes comprising a qLTC CSS code must also be locally testable

Let $\mathcal{C}(S_x, S_z)$ be a quantum CSS code corresponding to two linear codes $S_x^\perp, S_z^\perp \subseteq \mathbb{F}_2^n$. Suppose C is a qLTC, with parameter ρ . Then S_x^\perp and S_z^\perp are each LTCs with parameter at least $\rho/2$.

We now present a slight re-wording of the definition of LTC which would be useful later on:

Fact 10. The words of a residual LTC cluster around the original code

Let C be a locally testable code with parameter ρ . Any word w that violates at most ε fraction of the checks of C is at distance at most ε/ρ from C .

3 Local Hamiltonians with Approximation-Robust Entanglement

In [22] Freedman and Hastings defined an NLTS system as a local Hamiltonian, in which there are no easy-to-generate states with energy at most some ε -fraction of the total available energy of the system.

First, we will precisely define our model of quantum circuits. The following definition codifies some of the common-sense features of circuits that we will use.

Definition 11 (Circuits). A (unitary) quantum circuit C of depth d is a product of d layers U_1, \dots, U_d , where each layer U_i can be written as a tensor-product of 2-local unitary gates $U_{i,j}$:

$$U_i = \bigotimes_j U_{i,j} \quad (7)$$

Corresponding to a circuit C is a unitary operator U representing its action on an input state; often we will simply refer to U as a circuit when there is no ambiguity.

Low-depth circuits in turn imply a family of “simple” states, which we call trivial states (following [22]).

Definition 12 (Depth- d Trivial States). *We say that an n -qubit state ρ is depth- d trivial if it can be prepared by applying a depth- d quantum circuit to $|0\rangle^{\otimes N}$ (for some $N \geq n$) and tracing out $N - n$ qubits.*

Definition 13. No Low-Energy Trivial States (NLTS)

Let $\{H_n\}_{n \in \mathbb{N}}$ be a family of k -local Hamiltonians for $k = O(1)$. We say that $\{H_n\}_{n \in \mathbb{N}}$ is ε -NLTS if for any d and all sufficiently large n , any depth- d trivial state ρ satisfies

$$\text{tr}[\rho H_n] > \varepsilon. \quad (8)$$

We say that $\{H_n\}_{n \in \mathbb{N}}$ is NLTS if it is ε -NLTS for some constant $\varepsilon > 0$.

This definition was motivated, in part, to prevent the following form of NP-approximation of the ground-energy of such system: a prover sends a (polynomial-size) description of the shallow quantum circuit, and the verifier computes the expectation value of the Hamiltonian, conjugated by this unitary circuit, on the all-zero state. The verifier is thus able to accept/reject correctly, with high probability. Since the circuit has depth $O(1)$, and each term of H is local, each local term of UHU^\dagger is local, so this computation can be carried out efficiently. In general $\text{tr}[\rho H]$ can be estimated in time doubly exponential in d if d is a depth- d trivial state, since it requires estimating observables on neighborhoods of $O(2^d)$ qubits. (Similar but more complicated results hold when we replace a depth- d circuit with $e^{iH'}$ for H' a sum of local terms in which each qubit participates in interactions with total strength $O(d)$. [15, 38])

Conjecture 14 (NLTS conjecture [22]). *There exists a family of Hamiltonians with the NLTS property.*

In fact the original NLTS of Freedman and Hastings [22] was slightly weaker and considered only low-depth circuits in which the gates were restricted to have the same geometry as the Hamiltonian (see Definitions 1.1, 1.2, 1.3 of [22]). We consider a simpler and more general class of circuits in which any pairs of qubits can interact in each time step. Our main result is to prove a version of Conjecture 14 which is stronger in three ways.

1. As mentioned above, we rule out low-depth circuits including those with interactions between qubits that are far apart in the interaction graph defined by the Hamiltonian.
2. We show that low-depth circuits not only cannot produce low-energy states, they cannot even produce states that approximately match the classical probability distributions resulting from measuring these states in the X and Z bases.
3. We prove a depth lower bound that is not merely $\omega(1)$ but is $\Omega(\log(n))$. Since the naive algorithm for estimating expectation values runs in time doubly exponential in d , our results imply that this algorithm will require time exponential in some power of n .

Before stating our result formally, we define a stronger notion of non-triviality, called QNC¹-robustness. Recall that QNC¹ is the set of languages computable in quantum bounded-error log depth. We will use the term to describe classical distributions that can be approximately simulated with a quantum log-depth circuit.

Definition 15. QNC¹-hard distribution

A family of distributions $\{\mathcal{D}_n\}$ on n bits is said to be QNC¹-hard if there exist constants $\varepsilon, c > 0$ such that for sufficiently large n any depth- $c \cdot \log(n)$ trivial state ρ satisfies

$$\|\mathcal{D}_n - \text{diag}(\rho)\|_1 > \varepsilon. \quad (9)$$

Here $\text{diag}(\rho)$ can be thought of as the probability distribution resulting from measuring ρ in the computational basis.

Definition 16. QNC¹-hard quantum states

A family of n -qubit quantum states $|\psi_n\rangle$ is said to be QNC¹-hard if the corresponding family of distributions $\mathcal{D}_n(x) = |\langle x | \psi_n \rangle|^2$ is QNC¹-hard, where $|x\rangle$ denotes the standard computational basis.

Definition 17. QNC¹-hard local Hamiltonian

A local Hamiltonian H is said to be QNC¹-hard if any ground state of H is QNC¹-hard.

Definition 18. QNC¹-robust local Hamiltonian

A family of local Hamiltonians $\{H_n\}$ is QNC¹-robust if there exists $\varepsilon = \Omega(1)$ such that any family of quantum states $\{\rho_n\}$ satisfying $\text{tr}[H_n \rho_n] \leq \varepsilon$, is QNC¹-hard.

We can now state our main result.

Theorem 19. *There exists a family of QNC¹-robust $O(1)$ -local Hamiltonians.*

The NLTS conjecture of [22] follows as a corollary.

Most of the remainder of the paper is devoted to the proof of Theorem 19. In Section 4 we will prove that the probability distributions resulting from low-depth circuits cannot be approximately partitioned.

Then we will show that code states cannot be approximately partitioned. The canonical example of this is the cat state, as we mentioned in the introduction, and indeed it is well known that the cat state cannot be prepared in sub-logarithmic depth. In Section 5 we will prove a “warm-up” result showing that any Hamiltonian corresponding to a CSS code with $n^{\Omega(1)}$ distance is QNC¹-hard.

To find a QNC¹-robust Hamiltonian we will need a CSS code with stronger properties. In Section 6 we show that a qLTC (quantum locally testable code) gives rise to a QNC¹-robust Hamiltonian. While no qLTCs are known, the ideas here give a sense of how our full proof works. Our construction is described in Section 7, where the Tillich-Zémor hypergraph product from [41] is reviewed, and in Section 8 where we use it together with classical LTCs to construct our family of codes. Finally we prove that this family gives rise to QNC¹-robust Hamiltonians in Section 9.

4 Vertex expansion bounds for low-depth circuits

As stated above, the basic idea of this paper (following Lovett et al. [34]) is that distributions over codewords of good codes look very different from the outputs of low-depth circuits. We will see in this section that these can be distinguished by comparing the different values of vertex expansion that they induce on a particular graph.

Consider $\{0, 1\}^n$ to be the vertices of a graph with an edge between all pairs x, y with $\text{dist}(x, y) \leq \ell$. If $\ell = 1$ then this is the usual hypercube, but we will be interested in ℓ slightly larger than \sqrt{n} . For a set $S \subseteq \{0, 1\}^n$ define $\partial_\ell(S)$ to be the boundary of S , meaning points in S connected by an edge to a point in $S^c := \{0, 1\}^n - S$, along with points in S^c connected to a point in S . In other words

$$\partial_\ell(S) = \{x \in S : \exists y \in S^c, |x - y| \leq \ell\} \cup \{x \in S^c : \exists y \in S, |x - y| \leq \ell\}. \quad (10)$$

Let p be a probability distribution over $\{0, 1\}^n$. The p -weighted vertex expansion is defined to be

$$h_\ell(p) := \min_{0 < p(S) \leq \frac{1}{2}} \frac{p(\partial_\ell(S))}{p(S)}. \quad (11)$$

In this section we argue that the outputs of low-depth circuits have high vertex expansion for a suitable value of ℓ . To get intuition for this, we consider first the case of the uniform distribution over $\{0, 1\}^n$. Here Harper’s Theorem [25] implies that $h_\ell(\text{unif})$ is $\geq \Omega(1)$ when $\ell = \Omega(\sqrt{n})$. In fact it goes further and gives the exact isometric profile, meaning it calculates $\min_{p(S)=\mu} p(\partial_\ell(S) \setminus S)$ for all μ . Similar bounds are known for any product distribution p .

This can be extended to the case when p is the output of a classical depth- d circuit with m uniformly random input bits and fan-in, fan-out both ≤ 2 . In this case each output bit depends on $\leq 2^d$ bits. Suppose that C denotes the action of the circuit, $S \subset \{0, 1\}^n$ and $T := C^{-1}(S) \subseteq \{0, 1\}^m$. Then $p(S) = \text{unif}_m(T)$ where we define unif_m to be the uniform distribution on $\{0, 1\}^m$. Since the output can depend on $\leq n2^d$ bits of the input, we can assume without loss of generality that $n \leq m \leq n2^d$, or if d is constant then $m = \Theta(n)$. According to Harper's Theorem, if $\text{unif}_m(T) \leq 1/2$, x is drawn uniformly from T and z is drawn uniformly from the Hamming ball $\{|z| \leq \sqrt{m}\}$ then $x + z$ has $\Omega(1)$ probability of lying in T^c . Now we can use the assumption that the circuit is low depth to argue that

$$\text{dist}(C(x), C(x+z)) \leq |z|2^d \leq \sqrt{m}2^d \leq \sqrt{n}2^{1.5d}. \quad (12)$$

Since $C(x) \in S$ and $C(x+z) \in S^c$ this implies that $C(x) \in \partial_\ell(S)$ with $\ell = \sqrt{n}2^{1.5d}$. We conclude that $h_\ell(p) \geq \Omega(1)$. This argument is a restatement of Fact 4 from [20] (correcting a missing factor of \sqrt{n} there).

The main result of this section is to argue that a similar bound holds for the output of low-depth *quantum* circuits. We first formalize the fact that in sufficiently low depth circuits not all input bits can influence a given output bit.

Definition 20 (Light cone). *Given a depth- d quantum circuit C on n qubits we define a directed acyclic graph $G = (V, E)$ by considering $d+1$ layers of n vertices,*

$$V = \{V_0, \dots, V_d\}, |V_i| = n \quad \forall i \in \{0, \dots, d\}, \quad (13)$$

where V_0 correspond to the input qubits, and V_d correspond to the output qubits. Define the edge-set E by connecting for all $i \in [d]$, $k, l \in [n]$ the vertex $V_{i,k}$ to $V_{i+1,l}$ if there exists $C_{i,j}$ supported on qubits k, l . For a subset $S \subseteq V_d$ of output qubits, the light cone of S is defined as the set $L(S) \subseteq V_0$ of input qubits from which there exists a directed path to some vertex in S . The “blow-up” of a circuit is the maximum size of a light cone corresponding to a single output qubit.

For depth- d circuits comprised of k -qubit gates, the blow-up is $\leq k^d$. If the gates are required to be spatially local in D dimensions then this is $\leq (ckd)^D$ for some universal constant c depending on the specific geometry. In this paper we mostly are interested in the case of constant-depth circuits of two-qubit gates with unrestricted geometry, although our results hold more generally.

Theorem 21. *Let $|\psi\rangle = U|0^N\rangle$ for U a circuit with blow-up B . Let p be the probability distribution that results from measuring the first n qubits in the computational basis; i.e.*

$$p(x) = \sum_{y \in \{0,1\}^{N-n}} |\langle x, y | \psi \rangle|^2. \quad (14)$$

Then

$$h_\ell(p) \geq 0.56, \quad (15)$$

for $\ell = \sqrt{n}B^{1.5}$.

Our proof is inspired by the use of Chebyshev polynomials by Freedman and (the same!) Tillich [23] to relate the diameter of a graph to the spectral gap of its adjacency matrix, as well as by [8] to show that ground states of 1-d gapped Hamiltonians have bounded entanglement.

Proof. Define $\chi_S(x)$ to be -1 if $x \in S$ and 1 if not, and define the reflection operator

$$R = \sum_{\substack{x \in \{0,1\}^n \\ y \in \{0,1\}^{N-n}}} \chi_S(x) |x, y\rangle \langle x, y|. \quad (16)$$

Now define $|\psi'\rangle = R|\psi\rangle$. To gain intuition, if $|\psi\rangle$ is analogous to the cat state $(|0^N\rangle + |1^N\rangle)/\sqrt{2}$ then $|\psi'\rangle$ would be $(|0^N\rangle - |1^N\rangle)/\sqrt{2}$. Our proof strategy will be to construct an operator K such that

$$\langle\psi|K|\psi\rangle = 0 \quad (17a)$$

$$\langle\psi'|K|\psi'\rangle \leq 2.56p(\partial_\ell(S)) \quad (17b)$$

$$\langle\psi'|K|\psi'\rangle \geq 1.44p(S) \quad (17c)$$

Proving (17b) will require that K cannot detect the phase flip far from the boundary, while proving (17c) will require that K can nevertheless distinguish $|\psi\rangle$ from $|\psi'\rangle$.

Let $L \subseteq [N]$ denote the qubits in the light cone of $[n]$. By the definition of blow-up, $|L| \leq nB$. Define the Hamiltonians

$$H_0 = \frac{1}{|L|} \sum_{i \in L} |1\rangle\langle 1|_i \quad \text{and} \quad H = UH_0U^\dagger. \quad (18)$$

Note that H_0 can be thought of as the code Hamiltonian (cf. (4)) for the subspace with $|0\rangle$ for the qubits in L and arbitrary states elsewhere. Both H_0 and H have all eigenvalues between 0 and 1, both have a $2^{N-|L|}$ -fold degenerate ground space and both have gap $1/|L|$ to the first excited states above this. Define P_0 to project onto the states that are 0 in each of the qubits in L , i.e.

$$P_0 = |0\rangle\langle 0|^{\otimes L} \otimes I^{L^c}. \quad (19)$$

Similarly define $P = UP_0U^\dagger$. The idea of H_0 (resp. H) is to approximate $I - P_0$ (resp. $I - P$), and indeed they have the same 0-eigenspace. However, H_0 and H have other eigenvalues as small as $1/|L|$, making this a rather weak approximation. We will obtain a better approximation by taking polynomials of these operators, and will find that higher degree buys us a better approximation. Indeed $\lim_{m \rightarrow \infty} (I - H_0)^m = P_0$. But our proof will require the sharper degree/error tradeoff that comes from using Chebyshev polynomials, which we will see allows a degree of $\sqrt{|L|}$.

Let $m = \sqrt{nB}$. Following [8] we let $T_m(x)$ denote the degree- m Chebyshev polynomial which is $\cos(m \cos^{-1}(x))$ for $|x| \leq 1$ and $\cosh(m \cosh^{-1}(x))$ for $|x| \geq 1$. Additionally define

$$C_m(x) := 1 - \frac{T_m(f(x))}{T_m(f(0))}, \quad \text{where } f(x) := \frac{1 + \frac{1}{|L|} - 2x}{1 - \frac{1}{|L|}}. \quad (20)$$

Now we use Lemma 4.1 of [8] which states that:

$$C_m(0) = 0 \quad (21a)$$

$$C_m(x) \geq 1 - \frac{2}{e^2} \geq 0.72 \quad \text{for } \frac{1}{|L|} \leq x \leq 1 \quad (21b)$$

$$0 \leq C_m(x) \leq 1 + \frac{2}{e^2} \leq 1.28 \quad \text{for } 0 \leq x \leq 1 \quad (21c)$$

Define $K_0 = C_m(H_0)$ and $K = UK_0U^\dagger = C_m(H)$. Note that K_0 is m -local and K is ℓ -local for $\ell = Bm = \sqrt{nB}^{1.5}$. Since $C_m(H_0)$ consists only of powers of H_0 , it commutes with H_0 and can be evaluated by applying C_m to each eigenvalue of H_0 ; the same applies to $C_m(H)$ and H . Thus $0 \leq K \leq 1.28I$. By (21), the 0-eigenvalues of K are the same as the 0-eigenvalues of H and all the other eigenvalues of K are ≥ 0.72 . Thus we establish (17a) as well as the operator inequality

$$0.72(I - P) \leq K \leq 1.28(I - P). \quad (22)$$

Now we proceed to compute the upper and lower bounds on $\langle \psi' | K | \psi' \rangle$ claimed in (17). Partition $\{0, 1\}^N$ into four sets S_1, S_2, S_3, S_4 as follows:

$$S_1 = (S \setminus \partial_\ell(S)) \times \{0, 1\}^{N-n} \quad (23a)$$

$$S_2 = (S \cap \partial_\ell(S)) \times \{0, 1\}^{N-n} \quad (23b)$$

$$S_3 = (S^c \cap \partial_\ell(S)) \times \{0, 1\}^{N-n} \quad (23c)$$

$$S_4 = (S^c \setminus \partial_\ell(S)) \times \{0, 1\}^{N-n} \quad (23d)$$

Decompose $|\psi\rangle$ accordingly as

$$|\psi\rangle = |\psi_1\rangle + |\psi_2\rangle + |\psi_3\rangle + |\psi_4\rangle,$$

where the $|\psi_i\rangle$ are sub-normalized states having support in S_i . Note that $p(\partial_\ell(S)) = \|\psi_2\|^2 + \|\psi_3\|^2$. Using this notation we can write

$$|\psi'\rangle = -|\psi_1\rangle - |\psi_2\rangle + |\psi_3\rangle + |\psi_4\rangle.$$

Let $K_{ij} := \langle \psi_i | K | \psi_j \rangle$.

The fact that K is ℓ -local means that $K_{13} = K_{14} = K_{24} = 0$. Additionally (17a) means that $\sum_{i,j \in [4]} K_{ij} = 0$. Together these mean that

$$\langle \psi' | K | \psi' \rangle = -2K_{23} - 2K_{32} = -4\text{Re}K_{23}. \quad (24)$$

Since $\|K\| \leq 1.28$ we can use Cauchy-Schwarz to bound

$$|\langle \psi' | K | \psi' \rangle| \leq 5.12 \|\psi_2\| \cdot \|\psi_3\| \leq 2.56(\|\psi_2\|^2 + \|\psi_3\|^2) = 2.56p(\partial_\ell(S)), \quad (25)$$

thus establishing (17b).

We now turn to the proof of (17c). Observe that $U^\dagger R U$ acts only on the qubits in L . Thus $U^\dagger R U |0\rangle^{\otimes N} = U^\dagger R |\psi\rangle = U^\dagger |\psi'\rangle$ is a superposition of states of the form $|x\rangle^L \otimes |0\rangle^{L^c}$, implying that

$$P_0 U^\dagger |\psi'\rangle \propto |0\rangle^{\otimes N}.$$

We can determine the proportionality constant by calculating

$$\langle 0 |^{\otimes N} P_0 U^\dagger |\psi'\rangle = \langle 0 |^{\otimes N} U^\dagger |\psi'\rangle = \langle \psi | \psi' \rangle = \sum_x \chi_S(x) p(x) = 1 - 2p(S).$$

Thus $P_0 U^\dagger |\psi'\rangle = (1 - 2p(S)) |0\rangle^{\otimes N}$. We can then calculate

$$\langle \psi' | P | \psi' \rangle = \langle \psi' | U P_0 U^\dagger | \psi' \rangle \quad (26a)$$

$$= \langle \psi' | U (1 - 2p(S)) | 0 \rangle^{\otimes N} \quad (26b)$$

$$= (1 - 2p(S)) \langle \psi' | \psi \rangle \quad (26c)$$

$$= (1 - 2p(S))^2 \quad (26d)$$

Finally we can bound

$$\langle \psi' | K | \psi' \rangle \geq 0.72 \langle \psi' | (I - P) | \psi' \rangle \quad \text{using (22)} \quad (27a)$$

$$= 0.72(1 - (1 - 2p(S))^2) \quad (27b)$$

$$\geq 1.44p(S) \quad \text{using } p(S) \leq 1/2 \quad (27c)$$

□

Our proof of NLTS will require a slightly different graph property: upper bounds on the distance between large sets instead of lower bounds on the vertex expansion; i.e. showing that p cannot be approximately partitioned. The relation between these properties is a standard fact that does not involve any features of quantum circuits.

Corollary 22. *Let p be a probability distribution on n qubits generated by a quantum circuit with blow-up B , as in (14). If $S_1, S_2 \subset \{0, 1\}^n$ satisfy $p(S_1) \geq \mu$ and $p(S_2) \geq \mu$, then $\text{dist}(S_1, S_2) \leq 4\sqrt{n}B^{1.5}/\mu$.*

We refer to p with large well-separated sets as “approximately partitioned.” Roughly speaking Corollary 22 says that the outputs of low-depth circuits cannot be approximately partitioned.

Proof. Let $d = \text{dist}(S_1, S_2)$ and $\ell = \sqrt{n}B^{1.5}$. Assume $\mu \leq 1/2$, since otherwise we would have $d = 0$.

For $t = 0, 1, 2, \dots$ define the sets

$$U_t := \{x : (t-1)\ell < \text{dist}(x, S_1) \leq t\ell\}.$$

Then $S_1 = U_0$ and $S_2 \cap U_t = \emptyset$ for all $t < d/\ell$.

This implies that

$$\sum_{\substack{1 \leq t \leq \frac{d}{\ell} - 2 \\ t \text{ odd}}} p(U_t) + p(U_{t+1}) \leq 1 - 2\mu$$

and in turn that there exists a particular t_0 for which

$$p(U_{t_0}) + p(U_{t_0+1}) \leq \frac{1 - 2\mu}{\frac{d}{2\ell} - 1} \quad (28)$$

We will use t_0 to define a partition. Let

$$\bar{S}_1 = \bigcup_{t \leq t_0} U_t \quad \text{and} \quad \bar{S}_2 = \bigcup_{t > t_0} U_t.$$

Since $S_i \subseteq \bar{S}_i$ we have $p(\bar{S}_i) \geq \mu$ but now \bar{S}_1, \bar{S}_2 form a partition of $\{0, 1\}^n$. Thus by Theorem 21, $p(\partial_\ell(\bar{S}_1)) \geq 0.56\mu$. On the other hand $p(\partial_\ell(\bar{S}_1)) \leq p(U_{t_0}) + p(U_{t_0+1})$. From (28) we have

$$\frac{d}{2\ell} \leq 1 + \frac{1 - 2\mu}{0.56\mu} \leq 2\mu.$$

□

It should be straightforward to generalize Corollary 22 to arbitrary values of $p(S_1), p(S_2)$ along the lines of [23] but we do not pursue that here.

5 Warm-up: Quantum CSS Code-States are QNC¹-hard

In this section, we show that a natural sanity-check passes successfully, i.e. that quantum CSS codes cannot be sampled by bounded-depth circuits. We stress though, that such a claim is by no means robust. As mentioned before, known constructions of quantum CSS codes, despite having code-states that are not ε -hard for BD, for any $\varepsilon > 0$. This is mainly because these are physically-motivated constructions, and thus usually allow for embedding on a regular lattice of low-dimension. As an archetypal example, consider the 2-D Toric Code. The ε -residual code defined by discarding all check terms at the boundary of sufficiently large regular boxes cut out of the grid would allow local diagonalization of the residual code, and in particular, bounded-depth simulation. Our claim on quantum CSS codes is as follows:

Proposition 23. *Code-states of quantum CSS codes with linear distance are QNC¹-hard*
Let \mathcal{C} be a quantum CSS code on n qubits with $\Delta_{\min} = n^{1/2+\Omega(1)}$ and at least one logical qubit. Any $|\psi\rangle \in \mathcal{C}$ is QNC¹-hard.

We next present a version of the classic uncertainty principle [39] that implies that if two logical operators of a CSS codes anti-commute any state must have a high measure of “uncertainty” in at least one of these operators. This “sum” version is due to Hoffman and Takeuchi [29].

Lemma 24. *Let $|\psi\rangle$ be a quantum state, and A, B Hermitian observables satisfying $AB + BA = 0$ and $A^2 = B^2 = I$. Define*

$$\Delta A^2 = \langle \psi | A^2 | \psi \rangle - \langle \psi | A | \psi \rangle^2.$$

Then

$$\Delta A^2 + \Delta B^2 \geq 1. \quad (29)$$

Since the proof is short and our assumptions are slightly different from those of [29], we present a proof here.

Proof. Define the operator

$$C = \langle A \rangle A + \langle B \rangle B$$

where $\langle X \rangle := \langle \psi | X | \psi \rangle$. Define $\lambda \equiv \langle A \rangle^2 + \langle B \rangle^2$. Then we can directly calculate

$$C^2 = \lambda I \quad \text{and} \quad \langle C \rangle = \lambda \quad (30)$$

Thus $\lambda = \langle C \rangle \leq \sqrt{\langle C^2 \rangle} = \sqrt{\lambda}$, implying that $\lambda \leq 1$. Together with the fact that $\langle A^2 \rangle = \langle B^2 \rangle = 1$ this implies (29). \square

Next, we require a simple fact that can be found for example in [36] that any CSS code has a pair of bases, one for each of the quotient logical spaces, that anti-commute in pairs:

Fact 25. Anti-commuting checks

Let \mathcal{C} be a CSS code on n qubits: $\mathcal{C} = \mathcal{C}(S_x, S_z)$. There exist sets

$$\mathcal{B}_x = \{b_1^x, \dots, b_k^x\} \subset S_z^\perp \quad (31a)$$

$$\mathcal{B}_z = \{b_1^z, \dots, b_k^z\} \subset S_x^\perp \quad (31b)$$

such that $\{b_i^x + S_x\}_{i \in [k]}$ and $\{b_i^z + S_z\}_{i \in [k]}$ are bases for S_z^\perp / S_x and S_x^\perp / S_z respectively

$$\langle b_i^x, b_j^z \rangle = \delta_{j,k}. \quad (32)$$

Here we should think of $\{X^{b_i^x}\}$ and $\{Z^{b_i^z}\}$ as logical X and Z operators. We now prove that code states of QECCs with distance $n^{1/2+\Omega(1)}$ are QNC¹-hard.

Proof of Proposition 23. Let $|\psi\rangle$ be some code-state of \mathcal{C} . By Fact 25 above, one can find bases $\mathcal{B}_x, \mathcal{B}_z$ satisfying (32). Choose the first pair $b^x := b_1^x \in \mathcal{B}_x$, $b^z := b_1^z \in \mathcal{B}_z$ (any pair will work) and observe that according to Lemma 24 any state $|\psi\rangle$ will have

$$1 \leq (\Delta X^{b^x})^2 + (\Delta Z^{b^z})^2 = 2 - \langle X^{b^x} \rangle^2 - \langle Z^{b^z} \rangle^2.$$

and therefore either $|\langle X^{b^x} \rangle|$ or $|\langle Z^{b^z} \rangle|$ must be $\leq 1/\sqrt{2}$. Assume w.l.o.g. (since the other case is similar) that

$$|\langle Z^{b^z} \rangle| \leq 1/\sqrt{2}. \quad (33)$$

Let C_0 denote the linear space $\text{Span}(S_x^\perp - b^z) \subset \mathbb{F}_2^n$, and define the affine space $C_1 = C_0 + b^z$. If $s_0 \in C_0, s_1 \in C_1$ then $s_0 + s_1 \in (S_x^\perp - b^z) + b^z \subseteq S_x^\perp - S_z$, implying that $\text{wt}(s_0 + s_1) \geq \Delta_{\min}$. Since s_0, s_1 were arbitrary we conclude that

$$\text{dist}(C_0, C_1) \geq \Delta_{\min}. \quad (34)$$

Let \mathcal{D}_ψ denote the distribution on \mathbb{F}_2^n induced by measuring $|\psi\rangle$ in the tensor Z basis. Then (33) implies that

$$\mathcal{D}_\psi(C_0) \geq \frac{1}{2} - \frac{1}{2\sqrt{2}} \quad \text{and} \quad \mathcal{D}_\psi(C_1) \geq \frac{1}{2} - \frac{1}{2\sqrt{2}}. \quad (35)$$

Thus \mathcal{D}_ψ is approximately partitioned with parameter $(1/2 - 1/2\sqrt{2}, \Delta_{\min} = n^{1/2+\Omega(1)})$. Therefore, by Corollary 22 $|\psi\rangle$ is QNC¹-hard. \square

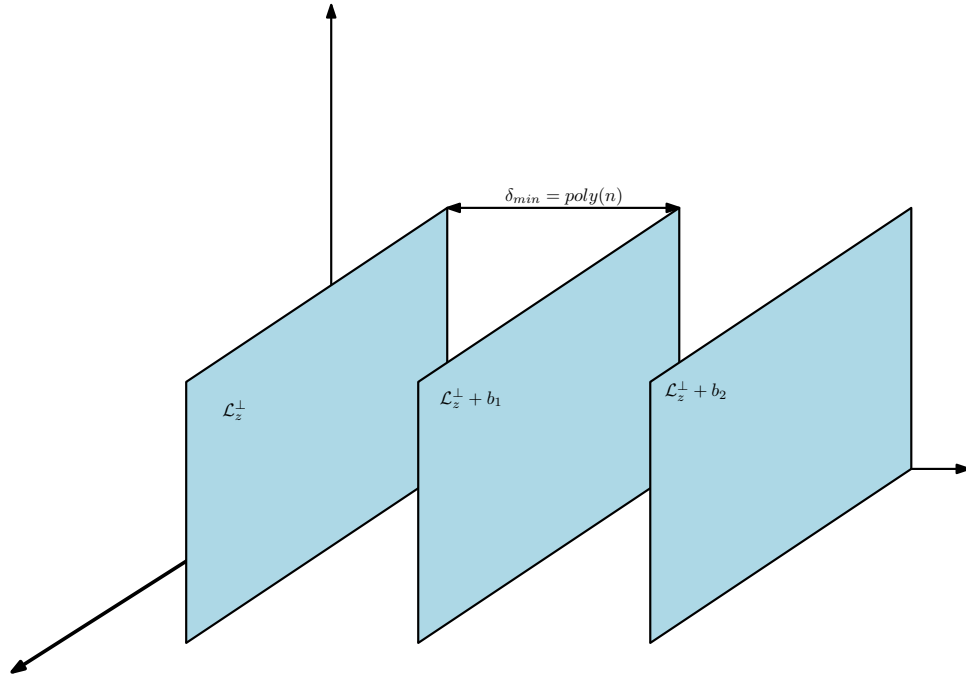


Figure 1: Depiction of the approximate partition of a quantum CSS code with large distance. Any code state must superpose non-negligibly in at least one of the two bases, on two distinct affine spaces separated by a large distance.

Implications for known quantum codes Proposition 23 yields a nontrivial bound on the quantum LDPC codes due to [21]. These codes are CSS codes and have distance $\Omega(\sqrt{n \log(n)})$ which corresponds to a circuit depth lower bound of $\Omega(\log \log(n))$.

One can also consider the Toric Code which has distance $\Theta(\sqrt{n})$. In such a case, while one cannot apply directly Proposition 23 - one can still show a similar proposition with a slightly relaxed definition of QNC¹-hardness, where the distribution is approximated to within distance $\varepsilon = n^{-1-\delta}$ for some constant $\delta > 0$. Indeed for any CSS LDPC code with distance $n^{\Omega(1)}$ we can show that approximating ground states to within distance $n^{-1-\Omega(1)}$ requires circuits of $\Omega(\log n)$ depth. We note that other methods are known [15, 27, 24] for showing that QECC ground states,

and even low-temperature thermal states of the 4-d toric code [26], are nontrivial. Indeed our proof can be viewed as a certain way of generalizing the argument of [15]. We provide a brief sketch of the proof here.

First we need a modified and indeed easier-to-prove version of Theorem 21. We claim that for $p(x)$ as in (14) we have

$$h_B(p) = \Omega(1/nB). \quad (36)$$

The proof is almost the same as that of Theorem 21 except that we skip the Chebyshev polynomial and simply set $K = H$. Then K is B -local and has a spectral gap of $\Omega(1/nB)$. We can then follow the same steps to show that for $|\psi\rangle, S, |\psi'\rangle$ defined as in Theorem 21 we have $\langle\psi|K|\psi\rangle = 0$, $\langle\psi'|K|\psi'\rangle = O(p(\partial_B S))$ and $\langle\psi'|K|\psi\rangle = \Omega(p(S)/nB)$. This establishes (36).

Next we follow the proof of Proposition 23 and construct the same pair of sets C_0, C_1 , with $D_\psi(C_0), D_\psi(C_1) \geq \Omega(1)$, where D_ψ is the probability distribution resulting from measuring a code state. Suppose that $\frac{1}{2}\|p - D_\psi\|_1 \leq \varepsilon = n^{-1-\Omega(1)}$. If $B = \Omega(\text{dist}(C_0, C_1)) = n^{\Omega(1)}$, then the circuit depth for ψ is $\Omega(\log(n))$ and we're done. Otherwise, assume $\text{dist}(C_0, C_1) > 2B$, and let S be the B -fattening of C_0 . Then $D_\psi(\partial_B(S)) = 0$, implying that $p(\partial_B(S)) \leq \varepsilon$. On the other hand, $p(S) = \Omega(1)$, so by (36) we have $p(\partial_B(S)) = \Omega(1/nB)$. Combining these we have $B = n^{\Omega(1)}$ which again implies the $\Omega(\log(n))$ circuit lower bound. We conclude that $\Omega(\log(n))$ -depth circuits are required to approximate code states to error $\leq n^{-1-\Omega(1)}$.

Non-CSS codes. It is tempting to speculate that Proposition 23 should hold for any quantum code (i.e. not only CSS) with distance $\omega(n^{1/2})$ and at least one logical qubit. While we believe this is likely to be true, we would need new techniques to prove it. It is possible for such codes to yield a nearly uniform distribution when measured in any local basis (e.g. consider a random 2-dimensional subspace of $(\mathbb{C}^2)^{\otimes n}$) which cannot be approximately partitioned. We note that using a proof similar to that of Proposition 23 one can show QNC¹-hardness for general stabilizer codes, but we omit this here for simplicity.

6 A bit further: Quantum locally testable codes are QNC¹-robust

We now connect between quantum locally testable codes (see definition of qLTC's in Definition 8) and local Hamiltonians with approximation-robust entanglement: For a qLTC with large minimal distance, all low-energy states for sufficiently small energy, yet constant as a function of system size, retain some non-negligible measure of long-range correlations from the entangled code-space of the code:

Theorem 26. *Let \mathcal{C} be a quantum locally testable CSS code with soundness $\rho > 0$, at least one logical qubit, and minimal distance $\Delta_{\min} \geq \Omega(n)$. Then \mathcal{C} is QNC¹-robust.*

While no codes are known that meet these conditions, the proof is conceptually a bridge between the proof of the exact case in Proposition 23 and our final proof of NLTS in Theorem 30.

Proof. Let $|\psi\rangle$ be some quantum state with:

$$\langle\psi|H(\mathcal{C})|\psi\rangle \leq \varepsilon, \quad (37)$$

for $\varepsilon > 0$ a constant we will choose later. The first part of the proof is the same as that of Proposition 23, although we initially consider a slightly different pair of subsets of \mathbb{F}_2^n . By Lemma 24 there exists a pair of logical operators $X^{b_1^x}, Z^{b_1^z}$ such that $|\psi\rangle$ has high uncertainty with respect to at least of those. Assume w.l.o.g. that $|\psi\rangle$ has high uncertainty w.r.t. Z^b where

$b := b_1^z$. Define $\tilde{C}_0 = \{b\}^\perp$ and $\tilde{C}_1 = b + C_0$. Note that \tilde{C}_0, \tilde{C}_1 partition \mathbb{F}_2^n . Then an argument along the lines of that leading up to (35) shows that

$$\mathcal{D}_\psi(\tilde{C}_0) \geq \frac{1}{2} - \frac{1}{2\sqrt{2}} \quad \text{and} \quad \mathcal{D}_\psi(\tilde{C}_1) \geq \frac{1}{2} - \frac{1}{2\sqrt{2}}, \quad (38)$$

where \mathcal{D}_ψ is the distribution over \mathbb{F}_2^n resulting from measuring $|\psi\rangle$ in the Z basis.

Now we cannot directly use the distance guarantees of the code since $|\psi\rangle$ is not necessarily a code state. However, by Fact 9, S_x^\perp is locally testable with parameter $\rho/2$. Moreover, by (37) the expected fraction of violated clauses in H_Z is $\leq 2\varepsilon$. Thus

$$\mathbb{E}_{z \sim \mathcal{D}_\psi} \text{dist}(z, S_X^\perp) \leq \frac{4\varepsilon n}{\rho} \quad (39)$$

$$\mathcal{D}_\psi(\{z : \text{dist}(z, S_X^\perp) \geq \frac{40\varepsilon n}{\rho}\}) \leq \frac{1}{10} \quad (40)$$

We now define

$$C_i = \{z \in \tilde{C}_i : \text{dist}(z, S_X^\perp) \leq 40\varepsilon n/\rho\}, \quad (41)$$

for $i = 0, 1$. By (38) and (40), we have $\mathcal{D}_\psi(C_i) \geq 1/2 - 1/2\sqrt{2} - 0.1 \geq 1/25$.

On the other hand, we will see that $\text{dist}(C_0, C_1)$ is large. If $s_0 \in C_0, s_1 \in C_1$ then we can write $s_i = t_i + u_i$ with $t_0, t_1 + b \in S_X^\perp - S_Z$ and $\text{wt}(u_i) \leq 40\varepsilon n/\rho$. The distance properties of the code guarantee that $\text{dist}(t_0, t_1) \geq \Delta_{\min}$. Then $\text{dist}(s_0, s_1) \geq \Delta_{\min} - 80\varepsilon n/\rho$. Since s_0, s_1 were arbitrary elements of C_0, C_1 we conclude that C_0, C_1 satisfy the same distance bound and thus that \mathcal{D}_ψ is approximately partitioned with parameter $(1/25, \Delta_{\min} - 80\varepsilon n/\rho)$. For sufficiently small $\varepsilon > 0$, Corollary 22 then implies an $\Omega(\log n)$ lower bound on the depth required to prepare $|\psi\rangle$. Thus \mathcal{C} is QNC¹-robust. \square

7 The Tillich-Zémor hypergraph product

In this section, we survey the Tillich-Zémor hypergraph product (TZ for short) introduced in [41]. We provide here only the very basic definitions that are required to prove our main theorem, and refer the reader to the original paper [41] for an in-depth view. The TZ-product code takes in two classical codes defined by their constraint Tanner graphs and generates a product of these graphs. Then it attaches a CSS code to the product graph. Formally stated:

Definition 27. The Tillich-Zémor hypergraph product

Given two codes defined by two bi-partite constraint graphs $\mathcal{C}_1 = (V_1, C_1), \mathcal{C}_2 = (V_2, C_2)$ the Tillich-Zémor product of these codes, denoted by

$$\mathcal{C}_\times = \mathcal{C}_1 \times_{TZ} \mathcal{C}_2,$$

is defined by the hypergraph product of the corresponding graphs. Its Hilbert space is comprised of qubits corresponding to

$$(V_1 \times V_2) \cup (C_1 \times C_2),$$

and check terms are of the following form:

$$H_x = C_1 \times V_2, H_z = V_1 \times C_2,$$

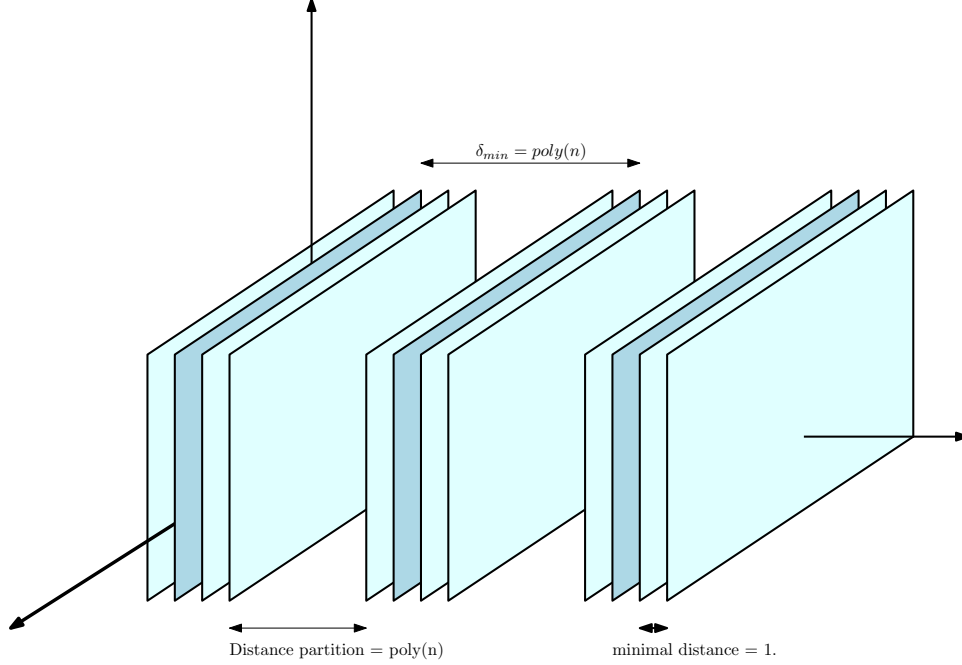


Figure 2: Robustness of qLTC entanglement: This shows the distribution of codewords (dark blue) and almost-codewords (light blue) for a qLTC. The codewords are separated by a large distance and the almost-codewords cluster near them. While the minimal “distance” within the set of almost-codewords can plummet to 1, by local testability, one can still find an approximate partition by “decoding” the new codewords back to the old code subspace.

The product $C_1 \times V_2$, for example, is interpreted in the following way: each constraint (c_1, v_2) is connected to all elements $(u, v_2) \in V_1 \times V_2$, where $u \in V_1$ is incident on check term $c_1 \in C_1$, and also, to all elements $(c_1, u) \in C_1 \times C_2$ where $u \in C_2$ is incident on bit $u \in V_2$. It follows from this definition that \mathcal{C}_\times is a CSS code $\mathcal{C}_\times(S_x, S_z)$, where as usual $S_x = \langle H_x \rangle$ and $S_z = \langle H_z \rangle$. For $|V_1| = n_1, |V_2| = n_2, |C_1| = m_1, |C_2| = m_2$, the code \mathcal{C}_\times is a quantum CSS code on $n_1 n_2 + m_1 m_2$ qubits, with $n_1 m_2 + n_2 m_1$ local checks.

We now state several useful facts on this construction, which can all be found in [41]. For a parity-check code \mathcal{C} given by its Tanner graph (V, C) we denote its transpose code \mathcal{C}^T as the parity check code whose Tanner graph is (C, V) . The following holds:

Fact 28. Properties of the Tillich-Zémor code[41]

1. If C_1, C_2 have locality parameters l_1, l_2, l_1^T, l_2^T , respectively, (l_1^T is the degree of each vertex $v \in V$ in the bi-partite Tanner graph of \mathcal{C}), then \mathcal{C}_\times has locality parameter $l_1 + l_2^T$ for H_x , and $l_2 + l_1^T$ for H_z .
2. $\delta_{\min}(\mathcal{C}_\times) \geq \min \{ \delta_{\min}(\mathcal{C}_1), \delta_{\min}(\mathcal{C}_2), \delta_{\min}(\mathcal{C}_1^T), \delta_{\min}(\mathcal{C}_2^T) \}$
3. Let $r(\mathcal{C})$ denote the number of qubits in a code \mathcal{C} . Then $r(\mathcal{C}_\times) = r(\mathcal{C}_1) \cdot r(\mathcal{C}_2) + r(\mathcal{C}_1^T) \cdot r(\mathcal{C}_2^T)$.

These logical operators of \mathcal{C}_\times can assume very complex forms, due in part, to the fact that the rate of the code scales like $r(\mathcal{C}_1) \cdot r(\mathcal{C}_2)$. Hence, the TZ-product of codes with linear rate is linear itself, i.e. scales like $\Omega(|V|^2)$. However, a particularly interesting subset of the logical operators, which is a subgroup w.r.t. addition modulo \mathbb{F}_2 , has a very succinct and useful form. We exploit the structure of this group to inherit, in some sense, the classical property of local testability.

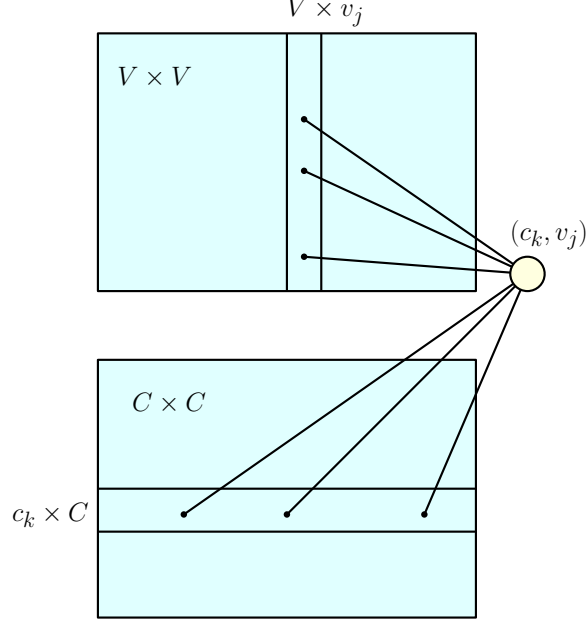


Figure 3: An example of a check term (c_k, v_j) of H_x . It is a parity check on all bits (v_m, v_j) in the j -th column of $V \times V$ such that v_m is examined by c_k in the original code \mathcal{C} , and on all bits in the k -th row of $C \times C$ that corresponds to checks incident on v_j in \mathcal{C} .

Fact 29. Group of logical operators isomorphic to the original code

For any $x \in \mathcal{C}_1$, and $y \notin \mathcal{C}_2^\perp$, the word

$$((x \otimes y)_{V_1 \times V_2}, 0_{C_1 \times C_2}) \in S_x^\perp - S_z$$

Similarly, for $x \notin \mathcal{C}_1^\perp$, $y \in \mathcal{C}_2$,

$$((x \otimes y)_{V_1 \times V_2}, 0_{C_1 \times C_2}) \in S_z^\perp - S_x.$$

Although we will not use this fact, one can also show that

$$(0_{V_1 \times V_2}, \mathcal{C}_2^T \otimes (\mathcal{C}_1^{T\perp})^c) \subset S_x^\perp - S_z$$

$$(0_{V_1 \times V_2}, (\mathcal{C}_2^{T\perp})^c \otimes \mathcal{C}_1^T) \subset S_z^\perp - S_x$$

In particular, if $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_1^T, \mathcal{C}_2^T$ are codes in which each bit appears at least once as 0 and once as 1 in some non-zero word, then

$$((\mathcal{C}_1 \otimes [n_2])_{V \times V}, 0_{C \times C}) \subset S_x^\perp - S_z \quad (42a)$$

$$([n_1] \otimes \mathcal{C}_2)_{V \times V}, 0_{C \times C}) \subset S_z^\perp - S_x \quad (42b)$$

The proof of this fact is straightforward and can be found in [41].

8 Explicit QNC¹-robust local Hamiltonians

In this section, we show how to construct QNC¹-robust local Hamiltonians based on CSS codes, but without using code distance directly. Our strategy will be to use the product code of Tillich-Zémor and show that low-energy states of the corresponding Hamiltonian can be approximately partitioned, implying (by Corollary 22) that they cannot be produced by low-depth

circuits. One subtlety is that we cannot look for an approximate partition using all of the bits of the code, since such a partition may not necessarily exist. This is because the T-Z (Tillich-Zémor) product allows to get codes on N qubits of distance at most $O(\sqrt{N})$ whereas our definition of low-energy allows errors on up to εN qubits. Instead we will show that an approximate partition exists on a subset of $O(\sqrt{N})$ qubits, which will be enough to yield our lower bound.

This is achieved by taking the T-Z product of a classical LTC with itself; i.e. $\mathcal{C}_\times = \mathcal{C} \times_{TZ} \mathcal{C}$ for \mathcal{C} an LTC. The resulting code \mathcal{C}_\times will in general not be a qLTC. However it can be thought of as a subsystem analogue for a qLTC. Namely, we will see that certain qubits of the low-energy states (those in $V \times V$) must either resemble code states of the underlying LTC or there must be detectable differences in some gauge-like qubits (those in $C \times C$).

Theorem 30. *There exists an explicit family of 7-local Hamiltonians $\{H^{(n)}\}_n$, where $H^{(n)}$ has at most $4n$ local terms, that are QNC¹-robust.*

8.1 The construction

Let n be a power of two. (We can always pad with dummy bits as well.) Let F be an expander graph on n vertices of degree 3. This exists via the construction of Lubotzky, Phillips and Sarnak [35].

8.1.1 Step 1: LTC with bounded-degree Tanner graph

Recall that the Hadamard code encodes $x \in \mathbb{F}_2^k$ as the $n := 2^k - 1$ -bit string whose entries are given by $x \cdot y$ for all $y \in \mathbb{F}_2^k - \{0\}$.

By the well-known affine test due to [12], there exists a set of 3-local parity checks that define the Hadamard code in a locally testable way. Explicitly, given the Hadamard code on \mathbb{F}_2^k , we consider the set of all parity checks of the form

$$T = \{f(x) + f(y) + f(x+y) | x, y \in \mathbb{F}_2^k, (x, y) \neq (0, 0)\},$$

where we define $f(0) := 0$. However, the Tanner graph $G_{\text{Had}} = (L, R; E)$, defined by these local checks, is such that the left degree (i.e. the degree of each bit) is $\binom{n}{2}/n$. Hence, by Fact 28 applying directly the Tillich-Zémor product to this graph, would generate a code with check terms whose locality is prohibitively large, i.e. scaling like a power of the number of qubits.

However, we claim that by essentially applying a degree-reduction procedure used in Dinur's combinatorial proof of the PCP theorem [19], we would get a locally testable code with constant left and right degrees. Let \mathcal{C} denote the degree-reduced Hadamard code, defined by the following operations on G_{Had} :

1. Replace each bit $x_i \in L$ with a cloud of bits X_i .
2. For each original test $t = f(x) + f(y) + f(x+y) \in R$, write it as a parity check on 3 unique variables x_y, y_x, z_x , where x_y is the y -th element of cloud X , y_x is the x -th element of cloud Y , and z_x is the x -th element of cloud $x+y$.
3. For each cloud X_i separately, add a set of equality constraints corresponding to the edges of the graph F .

The following facts can be readily shown on \mathcal{C} .

Fact 31.

1. \mathcal{C} is a binary parity-check code.
2. The Tanner graph of \mathcal{C} has bounded degree has left degree 4 and right degree at most 3.
3. \mathcal{C} is LTC with relative soundness $\rho > 0$, implying that \mathcal{C} has minimal relative distance $\delta_{\min} = \Omega(1)$.

4. Neither \mathcal{C} nor \mathcal{C}^T have constant bits - i.e. for each $0 \neq x \in \mathcal{C}, i \in V$, there exists $0 \neq y \in \mathcal{C}$ such that $x(i) \neq y(i)$.
5. \mathcal{C} is a code on n^2 bits with a number of checks $m = \binom{n}{2} + n^2 \cdot 3/2$.

To see why item 3 holds we use an argument similar to that of Lemma 4.1 of [19]. Note that now the encoded space consists of all words of the form w_1, \dots, w_n where each w_i is either all 0's or all 1's, and writing $b(w_i)$ as the bit of the i -th block implies that the n -bit string $b = (b(w_1), \dots, b(w_n))$ is a word in the original Hadamard code. Consider now the checks on \mathcal{C} . They are from two sets A, B of comparable size, where A consists of parity-checks on the expander graph in each w_i , and B applies the original Hadamard checks. Let $w = (w_1, \dots, w_n)$ be some word that is close to \mathcal{C} . Let $b' = (b'(w_1), \dots, b'(w_n))$ denote a bit-string in which we decide for each block w_i either 0 or 1 based on a *majority* vote. By definition of the expander graph repeating each bit of b' n times results in a word close to w . Since A and B have comparable sizes and the Hadamard is LTC then b' satisfies most checks of the original Hadamard code. Hence w is close to \mathcal{C} .

8.1.2 Step 2: TZ-Composition

Construct \mathcal{C}_\times as the Tillich-Zémor product of \mathcal{C} with itself, i.e.:

$$\mathcal{C}_\times = \mathcal{C} \times_{TZ} \mathcal{C}.$$

Denote by H_x, H_z the checks of \mathcal{C}_\times .

Fact 32. \mathcal{C}_\times is a code on registers $V \times V$ and $C \times C$, where $|V \times V| = n^4$ and $|C \times C| = m^2 + n^2 \leq 4n^4$. Furthermore, each check of H_x, H_z has support at most $d + 4 = 7$, and the number of check terms in each of H_x, H_z is at most $2n^4$.

We will see in the next section how these properties imply the QNC¹-robustness of $H(\mathcal{C})$.

9 Proof of NLTS

Proof of Theorem 30. Let \mathcal{C}_\times be the code defined in Section 8 and let $H = H(\mathcal{C}_\times)$ be the corresponding Hamiltonian.

Suppose that such a state $|\psi\rangle$ exists with $|\psi\rangle = U|0^N\rangle$ and U having depth d . Here $N \geq |V|^2 + |C|^2$ is the number of qubits which may include ancillas. For simplicity, we denote $|V| = n$ and $|C| = c \cdot n$, where c is the constant implicitly defined in Fact 31 above. We consider our Hamiltonian to act as identity on these ancillas. In what follows, define $\langle \cdot \rangle$ to mean $\langle \psi | \cdot | \psi \rangle$.

The proof has three components.

1. *Clustering of low-energy states.* Measuring low-energy states in either the X or Z bases will yield distributions for which all but $2\sqrt{\varepsilon}$ of the weight is on strings that satisfy a fraction at least $1 - \sqrt{\varepsilon}$ of the check operators.
2. *Uncertainty of logical operators.* For any pair of anti-commuting logical operators \bar{X}, \bar{Z} , and any state $|\psi\rangle$, at least one of the operators will have high uncertainty.
3. *Trivial states cannot be approximately partitioned.* Here we use Corollary 22 in the same way as in Proposition 23 and Theorem 26.

Clustering of low-energy states. We split up the terms in (4) by writing the code Hamiltonian as $H = \frac{H_X + H_Z}{2}$. When we consider the code construction from Section 8, H_X and H_Z

are given by:

$$H_X := \mathbb{E}_{j \in [n]} H_X^{(j)} \quad H_X^{(j)} := \frac{I}{2} + \frac{1}{2} \mathbb{E}_{c \in \mathcal{C}} \left(\prod_{i \in \Gamma(c)} X_{i,j}^V \right) \cdot \left(\prod_{c' \in \Gamma(j)} X_{c,c'}^C \right) \quad (43a)$$

$$H_Z := \mathbb{E}_{i \in [n]} H_Z^{(i)} \quad H_Z^{(i)} := \frac{I}{2} + \frac{1}{2} \mathbb{E}_{c \in \mathcal{C}} \left(\prod_{j \in \Gamma(c)} Z_{i,j}^V \right) \cdot \left(\prod_{c' \in \Gamma(i)} Z_{c',c}^C \right), \quad (43b)$$

where $\Gamma(\cdot)$ denote the set of neighbors of a variable or check, $X_{i,j}^V$ is a Pauli operator that is X on the (i, j) qubit of $V \times V$ and identity otherwise, and we define $Z_{i,j}^V$ similarly. $X_{i,j}^C$ is a Pauli operator that is X on the (i, j) qubit of $C \times C$ and identity otherwise, and similarly for $Z_{i,j}^C$.

Suppose that $|\psi\rangle$ is a low-energy state, namely:

$$\langle \psi | H | \psi \rangle \leq \varepsilon. \quad (44)$$

Then since the number of H_x, H_z terms are equal, then in particular:

$$\langle H_X \rangle = \mathbb{E}_{j \in [n]} \langle H_X^{(j)} \rangle \leq 2\varepsilon \quad \text{and} \quad \langle H_Z \rangle = \mathbb{E}_{i \in [n]} \langle H_Z^{(i)} \rangle \leq 2\varepsilon. \quad (45)$$

Define p_X, p_Z to be the probability distributions over $\{0, 1\}^N$ resulting from measuring every qubit of $|\psi\rangle$ in the X or Z bases respectively. Let $B_{X,\gamma}^{(j)}, B_{Z,\gamma}^{(i)}$ denote the sets of strings that violate a fraction at least $\gamma := 28\varepsilon$ of the constraints in $H_X^{(j)}, H_Z^{(i)}$, respectively.

From (45) we have that

$$\mathbb{E}_j p_X(B_{X,\gamma}^{(j)}) \leq \frac{2\varepsilon}{\gamma} \leq \frac{1}{14} \quad \text{and} \quad \mathbb{E}_i p_Z(B_{Z,\gamma}^{(i)}) \leq \frac{2\varepsilon}{\gamma} \leq \frac{1}{14}$$

Fix a pair $i, j \in [n]$ such that

$$p_X(B_{X,\gamma}^{(j)}) \leq \frac{1}{14} \quad \text{and} \quad p_Z(B_{Z,\gamma}^{(i)}) \leq \frac{1}{14} \quad (46)$$

Uncertainty of logical operators. Let $C_{\text{col}} \subseteq S_x^\perp - S_z, C_{\text{row}} \subseteq S_x^\perp - S_z$ denote the set of all logical operators of \mathcal{C}_\times of the special form of (42):

$$C_{\text{col}} \simeq \mathcal{C} \times [n], \quad C_{\text{row}} \simeq [n] \times \mathcal{C}. \quad (47)$$

For each $(i, j) \in [n] \times [n]$ there exists $x_i := x \otimes e_i \in C_{\text{row}}, z_j := e_j \otimes z \in C_{\text{col}}$ with $\langle x_i, z_j \rangle = 1$. To see this we need only choose x_i, z_j to both act nontrivially on the qubit (v_i, v_j) . This in turn requires that $\langle x, e_j \rangle = \langle z, e_i \rangle = 1$. This is possible because each bit is acted on nontrivially by some logical codeword in \mathcal{C} .

In what follows we will use the i, j from (46). Let X^{x_i} denote the Pauli operator corresponding to the logical word x_i , which is identity where x_i is 0 and X where x_i is 1. Let Z^{z_j} the Pauli operator corresponding z_j (replacing 1's with Pauli Z). These Pauli operators are supported only on $V \times V$, by definition.

By (29), for the state $|\psi\rangle$ (indeed for any state), we have

$$\Delta_{X^{x_i}}^2 + \Delta_{Z^{z_j}}^2 \geq 1,$$

so one of these must be $\geq 1/2$. Assume w.l.o.g. that $\Delta_{Z^{z_j}}^2 \geq 1/2$, and let \mathbf{B} be some basis of S_x^\perp / S_z containing z_j . Define $S_\pm \subseteq \mathbf{F}_2^n$ to be the sets of strings whose expansion by \mathbf{B} contains / does not contain z_j . Then by the above

$$p_Z(S_-) \geq 1/2 - 1/\sqrt{2}, \quad p_Z(S_+) \geq 1/2 - 1/\sqrt{2} \quad (48)$$

Simultaneous uncertainty and clustering Define $S_{\pm}^G = S_{\pm} - B_{Z,\gamma}^{(i)}$. Observe that

$$\{0, 1\}^n = S_+^G \sqcup S_-^G \sqcup B_{Z\sqrt{\varepsilon}}^{(i)}. \quad (49)$$

Thus we can write

$$\psi = |\psi_+\rangle + |\psi_-\rangle + |\psi_B\rangle, \quad (50)$$

for orthogonal sub-normalized states $|\psi_+\rangle, |\psi_-\rangle, |\psi_B\rangle$ with supports contained respectively within $S_+^G, S_-^G, B_{Z\sqrt{\varepsilon}}^{(i)}$. By our earlier arguments $\langle \psi_B | \psi_B \rangle \leq 2\varepsilon/\gamma$ and therefore $\langle \psi_{\pm} | \psi_{\pm} \rangle \geq 1/2 - 1/2\sqrt{2} - 2\varepsilon/\gamma \geq \frac{1}{14}$.

By Corollary 22, to prove that p_Z cannot result from a circuit of depth $o(\log(n))$ it is sufficient to find a subset T of $\Omega(n)$ bits such that for any $x \in S_+^G, y \in S_-^G$ we have $\text{dist}(x|_T, y|_T) = \Omega(|T|)$.

Define R_1, R_2 to be the maps that given $i \in [n]$ restrict $\{0, 1\}^N$ to $\{0, 1\}^{\{i\} \times V}$ and $\{0, 1\}^{\Gamma(\{i\} \times V)}$ respectively. Here we define $\Gamma(\{i\} \times V)$ to be the locations in $C \times C$ that share checks with $\{i\} \times V$; explicitly

$$\Gamma(\{i\} \times V) = \Gamma(\{i\}) \times C.$$

Note that in the original code \mathcal{C} the checks were of the form $\langle c, x \rangle = 0$ and in the product code \mathcal{C}_{\times} , they are of the form $\langle c, R_1(x) \rangle = \langle c', R_2(x) \rangle$ for appropriate pairs of checks $c \in \mathcal{C}, c' \in \mathcal{C}^T$. Let $R(x) := (R_1(x), R_2(x))$. Observe that the output of R consists of $n + cn$ bits. We claim that

$$\text{dist}(R(S_+^G), R(S_-^G)) = \Omega(n). \quad (51)$$

Let $x \in S_+^G, y \in S_-^G$, and consider their difference modulo 2: $z = x + y$. Put

$$\eta \equiv \frac{1}{n} \text{wt}(R_2(z)). \quad (52)$$

Each element of the set $R_2(i)$ is examined by a unique element of $H_Z^{(i)}$. Hence, $\langle c', R_2(z) \rangle = 0$ for at most ηn check terms.

In addition, by assumption $x, y \notin B_{Z,\gamma}^{(i)}$ and therefore z violates at most $2\gamma cn$ checks of $H_Z^{(i)}$. Accumulating these two contributions implies that $\langle c, R_1(x + y) \rangle = 1$ for at most $2\gamma cn + \eta n$ checks. By the LTC condition (Definition 6),

$$\frac{1}{n} \text{dist}(R_1(z), \mathcal{C}) \leq \frac{56c\varepsilon + \eta}{\rho}.$$

The fact that $R_1(z)$ is close to the original code is insufficient, for it may be that it is very close to the 0 word. At this point, the uncertainty principle is invoked. We claim that z must be close to a *non-zero* word of \mathcal{C} : Indeed, $z = x + y$, where $x \in S_+^G, y \in S_-^G$ hence z , when expressed by a basis \mathbf{B} containing z_i is spanned also by z_i . Therefore:

$$\text{wt}(R_1(x + y)) \geq n(\delta - \frac{56c\varepsilon + \eta}{\rho}). \quad (53)$$

Optimizing the value of η in Equations 53, 52 we get an $\Omega(n)$ lower bound on the distance. \square

10 Acknowledgements

We thank Dorit Aharonov, and Jeongwan Haah for useful conversations, Fernando Brandão, Toby Cubitt, Isaac Kim, Anthony Leverrier and Cedric Lin for useful and detailed comments and Alex Lubotzky for pointing out the fundamental importance of the Tillich-Zémor construction. We are both funded by the Templeton foundation and AWH is funded by NSF grants CCF-1111382 and CCF-1452616 and ARO contract W911NF-12-1-0486.

References

- [1] S. Aaronson. The quantum PCP manifesto. Blog: “Shtetl-Optimized”.
- [2] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A*, 70:052328, 2004, arXiv:quant-ph/0406196.
- [3] D. Aharonov, I. Arad, Z. Landau, and U. Vazirani. The detectability lemma and quantum gap amplification. In *STOC '09*, pages 417–426, 2009, arXiv:0811.3412.
- [4] D. Aharonov, I. Arad, and T. Vidick. Guest column: The quantum PCP conjecture. *SIGACT News*, 44(2):47–79, June 2013, arXiv:1309.7495.
- [5] D. Aharonov and L. Eldar. On the complexity of commuting local Hamiltonians, and tight conditions for topological order in such systems. In *FOCS '11*, pages 334–343, 2011, arXiv:1102.0770.
- [6] D. Aharonov and L. Eldar. Quantum locally testable codes, 2013, arXiv:1310.5664. to appear in SICOMP.
- [7] D. Aharonov and L. Eldar. The commuting local Hamiltonian problem on locally expanding graphs is approximable in NP. *Quantum Information Processing*, 14(1):83–101, Jan. 2015, arXiv:1311.7378.
- [8] I. Arad, A. Kitaev, Z. Landau, and U. Vazirani. An area law and sub-exponential algorithm for 1D systems. In *Proceedings of the 4th Innovations in Theoretical Computer Science (ITCS)*, 2013, arXiv:1301.1162.
- [9] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *JACM*, 45(3):501–555, 1998.
- [10] S. Arora and S. Safra. Probabilistic checking of proofs: A new characterization of NP. *JACM*, 45(1):70–122, 1998.
- [11] E. Ben-Sasson, P. Harsha, and S. Raskhodnikova. Some 3cnf properties are hard to test. *SIAM Journal on Computing*, 35(1):1–21, 2005.
- [12] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *Journal of Computer and System Sciences*, 47(3):549–595, 1993.
- [13] F. G. S. L. Brandão and A. W. Harrow. Product-state approximations to quantum ground states. In *Proceedings of the 45th annual ACM Symposium on theory of computing*, STOC '13, pages 871–880, 2013, arXiv:1310.0017.
- [14] F. G. S. L. Brandão, A. W. Harrow, and M. Horodecki. Local random quantum circuits are approximate polynomial-designs, 2012, arXiv:1208.0692.
- [15] S. Bravyi, M. Hastings, and F. Verstraete. Lieb-robinson bounds and the generation of correlations and topological quantum order. *Phys. Rev. Lett.*, 97:050401, 2006. arXiv:quant-ph/0603121.
- [16] S. Bravyi and M. Vyalii. Commutative version of the local Hamiltonian problem and common eigenspace problem. *Quantum Inf. Comput.*, 5(3):187–215, May 2005, arXiv:quant-ph/0308021.
- [17] J. Chen, Z. Ji, B. Zeng, and D. L. Zhou. From ground states to local hamiltonians. *Phys. Rev. A*, 86:022339, Aug 2012, arXiv:1110.6583.
- [18] X. Chen, Z.-C. Gu, and X.-G. Wen. Local unitary transformation, long-range quantum entanglement, wave function renormalization, and topological order. *Phys. Rev. B*, 82:155138, Oct 2010, arXiv:1004.3835.
- [19] I. Dinur. The PCP theorem by gap amplification. *JACM*, 54(3):12, 2007.

- [20] L. Eldar. Local hamiltonians with approximation-robust entanglement, 2015, arXiv:1503.02269.
- [21] M. Freedman, D. Meyer, and F. Luo. \mathbb{Z}_2 -systolic freedom and quantum codes. In R. K. Brylinski and G. Chen, editors, *Math. of Quantum Computation*, pages 287–320. Chapman & Hall/CRC, 2002.
- [22] M. H. Freedman and M. B. Hastings. Quantum systems on non- k -hyperfinite complexes: A generalization of classical statistical mechanics on expander graphs, Jan. 2014, arXiv:1301.1363.
- [23] J. Friedman and J.-P. Tillich. Laplacian eigenvalues and distances between subsets of a manifold. *J. Differential Geom.*, 56(2):285–299, 10 2000.
- [24] J. Haah. An invariant of topologically ordered states under local unitary transformations, 2014, arXiv:1407.2926.
- [25] L. H. Harper. Optimal assignments of numbers to vertices. *Journal of the Society for Industrial and Applied Mathematics*, 12(1):131–135, 1964.
- [26] M. Hastings. Topological order at non-zero temperature. *Phys. Rev. Lett.*, 107:210501, 2011, arXiv:1106.6026.
- [27] M. B. Hastings. Locality in quantum systems, 2010, arXiv:1008.5137. lecture notes from Les Houches summer school.
- [28] M. B. Hastings. Trivial low energy states for commuting Hamiltonians, and the quantum PCP conjecture, 2012, arXiv:1201.3387.
- [29] H. F. Hofmann and S. Takeuchi. Violation of local uncertainty relations as a signature of entanglement. *Phys. Rev. A*, 68:032103, Sep 2003, arXiv:quant-ph/0212090.
- [30] I. H. Kim. On the informational completeness of local observables, 2014, arXiv:1405.0137.
- [31] A. Kitaev. On the classification of short-range entangled states, 2013. <http://scgp.stonybrook.edu/archives/7874>.
- [32] A. Y. Kitaev, A. H. Shen, and M. N. Vyalyi. *Classical and Quantum Computation*, volume 47 of *Graduate Studies in Mathematics*. AMS, 2002.
- [33] A. Leverrier, J.-P. Tillich, and G. Zémor. Quantum expander codes, 2015, arXiv:1504.00822. to appear in FOCS 2015.
- [34] S. Lovett and E. Viola. Bounded-depth circuits cannot sample good codes. *Computational Complexity*, 21(2):245–266, 2012.
- [35] A. Lubotzky, R. Phillips, and P. Sarnak. Ramanujan graphs. *Combinatorica*, 8(3):261–277, 1988.
- [36] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, New York, 2000.
- [37] T. Osborne. Hamiltonian complexity, 2011, arXiv:1106.5875.
- [38] T. J. Osborne. Efficient approximation of the dynamics of one-dimensional quantum spin systems. *Phys. Rev. Lett.*, 97:157202, Oct 2006, arXiv:quant-ph/0508031.
- [39] H. P. Robertson. The uncertainty principle. *Phys. Rev.*, 34:163–164, Jul 1929.
- [40] B. Swingle and J. McGreevy. Renormalization group constructions of topological quantum liquids and beyond, 2014, arXiv:1407.8203.
- [41] J.-P. Tillich and G. Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to $n^{1/2}$. In *Proceedings of the 2009 IEEE international conference on Symposium on Information Theory - Volume 2*, ISIT’09, pages 799–803, 2009, arXiv:0903.0566.
- [42] J. Watrous. Quantum computational complexity, 2008, arXiv:0804.3401.